Evan A. Schmutz (3860)
kima@hjslaw.com
Wm. Kelly Nash (4888)
wmkellynash@aol.com
Jordan K. Cameron (12051)
jcameron@hjslaw.com
HILL, JOHNSON & SCHMUTZ, L.C.
River View Plaza, Suite 300
4844 North 300 West
Provo, Utah 84604
Telephone: (801) 375-6600
Fax: (801) 375-3865

Attorneys for Plaintiff ZooBuh, Inc.

UNITED STATES DISTRICT COURT

DISTRICT OF UTAH, CENTRAL DIVISION

ZOOBUH, INC., a Utah Corporation, Plaintiff, vs. BETTER BROADCASTING, LLC., a Utah limited liability company; IONO INTERACTIVE, a company doing business in Utah; DOES 1-40, Defendants.	**MEMORANDUM IN SUPPORT OF MOTION TO ENTER ORDER AND MEMORANDUM RE STANDING AND DAMAGES** Case No.: 2:11cv00516-DN Judge David O. Nuffer

Plaintiff ZooBuh, Inc. ("**ZooBuh**") by and through its counsel of record, hereby submits this Memorandum in Support of Motion to Enter Order and Memorandum re Standing and

Damages, together with the supporting Declaration of Alan Fullmer (Dkt 43), Declaration of Bryceson Ringwood (Dkt 42), and Expert Letter of Opinion (Dkt 38).

Introduction

ZooBuh alleges in its Complaint that Defendants Better Broadcasting, LLC and IONO Interactive (collectively "**Defendants**") transmitted thousands of commercial email messages in violation of the federal CAN-SPAM act of 2003, 15 U.S.C. § 7701 *et seq*. ("CAN-SPAM").

In summary, CAN-SPAM prohibits sending unauthorized commercial email with header information that is materially false or materially misleading. Additionally, CAN-SPAM requires that specific disclosures and other identifying information appear in the body of the emails. The emails in this case contain significant violations of the CAN-SPAM Act which subject the Defendants to statutory penalties as outlined in 15 U.S.C. § 7706(g)(3)(A).

Statement of Facts

Procedural History

1. On November 29, 2011, ZooBuh, by order of this Court, served a Complaint and Summons on Better Broadcasting and IONO Interactive via mail at 363 No. University Ave., Suite 110, Provo, Utah 84601.

2. The Defendants failed to respond to the Complaint and Summons.

3. On March 07, 2012, this Court entered Default Judgment against both Defendants.

ZooBuh is a Bona Fide Internet Access Service

4. ZooBuh was first formed in 2002. (Declaration of Alan Fullmer, ¶ 3, lodged as Dkt. 43, "**Fullmer Decl.**").

5. ZooBuh offers email services, blog hosting, and chat services. (*Id*. at ¶ 4).

6. On Jan 22, 2007, ZooBuh incorporated in the state of Utah. (*Id*. at ¶ 5).

7. ZooBuh is a widely and well recognized service provider of email, blog, and chat services. ZooBuh has been featured in articles published in *PC Advisor*, *PC Magazine*, *Tech World, The Guardian, Find it Quick Internet Guide*, *Yahoo's Associated Content* and has been mentioned in the following books: How to Protect Your Children on the Internet, by Gregory S. Smith; and, CyberSafety, by Ken Knapton. ZooBuh has also been mentioned and/or featured on KSL News' Nanny Radio Show and WBTV. (*Id*. at ¶ 6).

8. ZooBuh has customers in all 50 states and in 27 different countries. (*Id*. at ¶ 7).

9. ZooBuh services approximately 35,000 customer accounts. (*Id*. at ¶ 8).

10. ZooBuh owns all the servers, routers, and switches on its network through which it hosts and provides its internet access services for its customers. (*Id*. at ¶ 12).

11. As of December 2011, ZooBuh had three employees and ran its services on a network of eight servers, four of which would be completely unnecessary but for the continuous onslaught of unlawful commercial emails (more commonly known as SPAM) sent to ZooBuh's servers. (*Id*. at ¶ 11).

12. Every ZooBuh email account is registered, hosted, and serviced through ZooBuh's own hardware. ZooBuh also provides each of its customers with their own web-based email portal through which they access their selected web based services (e.g. email, blogs, chat.). (*Id*. at ¶¶ 13-14).

13. ZooBuh stores the routers, switches, and servers in a leased space which offers storage space, redundant Internet connections, physical security, and climate control. (*Id*. at ¶ 15).

14. ZooBuh has sole ownership of all the hardware (i.e., servers, routers, switched, etc.), complete and uninhibited access to the hardware, and sole physical control over the hardware through which it offers its access service. (*Id*. at ¶ 16).

ZooBuh is adversely affected by unlawful commercial emails ("SPAM").

15. In its ordinary course of business, ZooBuh utilizes SpamHaus, Razor, Pyzor and Spamassassin as a first line of defense for SPAM email that arrives on its system. (*Id*. at ¶ 17).

16. In 2011 ZooBuh also expended significant time to develop, design, and code a proprietary SPAM filtering and behavior categorizing software that it implemented on its system as a way to better deal with its ongoing conflict with unlawful commercial email. (*See id*. at ¶¶ 18-19).

17. Though current first line systems such as Spamassassin successfully flag and discard many SPAM messages, ZooBuh has found that spamming techniques evolve faster than does the security. For this reason, there is a window where publicly available honeypots (a process set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems) and SPAM lists do not include the newest threats. The result is a constant battle with unlawful commercial email that takes significant time, money and resources above and beyond the implementation of commercial SPAM filters, which ZooBuh has done. (*Id*. at ¶ 20).

18. In order to deal with unlawful commercial email in a way that limits the damaging effects that SPAM has on ZooBuh's business, ZooBuh is constantly expending employee time to update its proprietary software to identify new spamming trends, and styles, all for the purpose of preventing the unwanted messages from entering and damaging ZooBuh's system. (*Id*. at ¶ 21).

19. Currently about 70% of the email messages that ZooBuh receives on its system are unlawful commercial emails. This number would be significantly higher if not for all the precautions that ZooBuh has taken. (*Id*. at ¶ 24).

20. Email marketers, such as Defendants, create infinite numbers of internet domains from which to send unlawful emails, none of which accurately identify any party, and in some cases, are not domain names that actually exist. These types of tricks, which alter the header information in an email message, help the emails to evade blacklists, SPAM filters, and help the emails find their way onto ZooBuh's system. (*Id*. at ¶ 26).

21. The majority of the unlawful commercial emails that ZooBuh's servers receive use false or misleading header/transmission information. These types of emails harm ZooBuh's system, require constant monitoring, updates, extra work, etc. (*Id.* at ¶ 22). The emails in this case fall into this category. (Declaration of Bryceson Ringwood, ¶¶ 8-11, lodged as Dkt. 42, "**Ringwood Decl.**").

22. As a result of SPAM, including the emails in question, ZooBuh has had to consistently increase the size and servicing capacity of its system, despite no significant growth to its customer base (ZooBuh has fluctuated between 30,000 and 35,000 customer accounts over the past two years). (Fullmer Decl. at ¶¶ 10, 29).

23. With each added server, ZooBuh also has had to increase its bandwidth in order to service the new space adequately. (*Id*. at ¶ 29).

24. Even with eight servers, ZooBuh consistently deals with server spikes and crashes, and the servers are constantly pushed to capacity, which significantly decreases the life span of the servers and is expensive in power consumption. (*Id*. at ¶ 30).

25. Specifically, as the result of its receipt of unlawful commercial emails,

a. in May 2011, ZooBuh experienced a primary DNS server overload which caused a crash and a bandwidth spike resulting in an 1800% increase above average usage. (*Id*. at ¶ 38(a)).

b. In June 2011, ZooBuh experienced a Mail server overload, which resulted in extremely slow delivery of legitimate emails and an eventual memory exhaustion which ended in an unrecoverable kernel crash[1]. (*Id*. at ¶¶32(a), 36(b)).

c. In July 2011, ZooBuh was the victim of a massive spam attack, resulting in a server spike and eventual crash, which caused delayed delivery of legitimate emails. (*Id*. at ¶ 36(c)).

d. In August 2011, ZooBuh was again the victim of a massive spam attack, resulting in a server spike which caused delayed delivery of legitimate emails. (*Id*. at ¶ 32(c)).

[1] A kernel crash is an actual loss of use of hardware and data and is unrecoverable. It requires manual physical intervention to restore the hardware to operating functionality. Further testing and log evaluation is also required to pinpoint these causes. This always results in loss of productivity and processing capability of a business.

26. On average, all of ZooBuh's servers are constantly running above their recommended capacity due to the continuous onslaught of unlawful commercial emails. (*Id*. at ¶33).

27. None of these spikes, crashes or delays would have occurred but for the unlawful commercial emails, and the spikes, crashes or delays occurred despite ZooBuh's taking significant precautionary measures, such as implementing and constantly updating SPAM filters. (*Id*. at ¶ 39).

28. Due to the number of unlawful emails sent to ZooBuh recipients during the time frame of the Better Broadcasting emails, ZooBuh has had to increase its capacity from four to eight servers, all at significant expenses to ZooBuh. (*Id*. at ¶ 40).

29. Additionally, ZooBuh, on a fairly regular basis, receives customer complaints attributable to SPAM. In essence, the customers complain that their email is not being delivered and/or received promptly, and that the system runs slowly overall. ZooBuh can state with certainty that the slowdown issues complained of are directly attributable to ZooBuh's receipt of the unlawful email. (*Id*. at ¶ 42).

30. The harm suffered by ZooBuh on a regular basis is much more significant than the mere annoyance of having to deal with SPAM or the process of dealing with SPAM in the ordinary course of business (i.e. installing a spam filter to flag and discard SPAM). (*Id*. at ¶ 43).

31. The harm ZooBuh suffers is manifested in significant financial expense and burden, significant loss of employee time, significant loss in profitability and ability to grow the company, significant decreases in the life span of ZooBuh's hardware, which ultimately will

result in more spikes, more crashes, and pre-mature hardware replacements and more money. (*Id*. at ¶¶ 40-44).

ZooBuh was adversely affected by the SPAM in question.

32. From around February 18, 2011 to November 7, 2011, ZooBuh received at least 13,453 commercial emails sent and/or initiated by or on behalf of Better Broadcasting and/or Iono, its alter ego. (*Id*. at ¶ 45).

33. During the time frame that the emails in question were received, ZooBuh had to increase its network from four to eight servers and perform many of the upgrades identified above. (*Id*. at ¶ 40).

34. For each individual email, ZooBuh had to expend man hours and work to identify the source of the email, to determine how and why the specific emails were able to circumvent and/or bypass preliminary filtering techniques, and ultimately to make the emails stop. (*Id*. at ¶¶ 55-66; Ringwood Decl., at ¶¶ 2-12).

35. Specifically, for each individual email, ZooBuh expended man hours in examining the transmission information of the email, examining and analyzing the header information of the email, and examining the content and MIME data of the email. (Fullmer Decl. ¶ 65).

36. ZooBuh also had to expend man hours to trace each of the individual sender domains in an effort to determine if the domain was legitimate, registered, cloaked, or otherwise identified the sending party. (*Id*. at ¶ 66; Ringwood Decl., at ¶¶ 2-12).

37. ZooBuh also had to retain counsel to examine the emails for violations of applicable laws and to expend effort to getting the emails in question to stop. (Fullmer Decl. at ¶ 67).

The Emails Contain CAN-SPAM Violations

38. When an email arrived on ZooBuh's servers, the original file is duplicated and one copy is stored on a secure, read only server, as a backup. The other copy is transmitted to the intended recipient. (*Id*. at ¶ 46).

39. ZooBuh's system assigns each email a unique control ID number, for purposes of cataloging and organizing the emails. (*Id*. at ¶ 47).

40. Mr. Fullmer personally extracted the pertinent "header" information from each email in this case and provided it to an employee, Mr. Bryceson Ringwood ("**Mr. Ringwood**), with assignment to examine the publicly available WHOIS information of the domains in question as it existed for each on the specific dates of each of the emails in question. (*See Id*. at ¶¶ 55-58; *see* Ringwood Decl. at ¶¶ 5-12).

41. WHOIS history information contains the registration dates of the domain names, identifies the domain registrar, and indicates if the domain is privacy protected or public. One can also determine, based on the registration dates, if a specific domain was not registered when a specific email was sent. (Ringwood Decl. at ¶ 7).

42. With the information provided by Mr. Fullmer, Mr. Ringwood examined the WHOIS history for each email in question and determined that 13,333 of emails contained a generic "from" name and were transmitted from privacy protected domain names. (*Id*. at ¶ 9).

43. Mr. Ringwood also determined that 13,452 of the emails were transmitted from domains registered with eNom and that one of the emails was transmitted from a domain registered with Moniker. (*See id*. at ¶ 10).

44. With this information, Mr. Ringwood compiled a Domain Check Report which summarizes his findings and includes the sender domain, the domain registrar, the Control ID number of the email, the date of the email, the domain registration status, and a citation to the appropriate WHOIS domain history record. (*Id*. at ¶¶ 11).

45. When ZooBuh sought to identify the emailer through the publicly available WHOIS database, the WHOIS database record displayed the proxy service's contact information on the domain name registration records instead of the emailer's contact information, thereby preventing ZooBuh from identifying the emailer. (*Id*. at ¶¶ 8-9).

46. The emails in question also fail to contain an advertisement notice and unsubscribe notice that would reasonably be viewed by the recipient of the email. (*See* Letter of Opinion of F. Alan Fullmer at ¶¶ 61-65, 67-70, lodged as Dkt. 38, "**Letter of Opinion**").

47. Additionally, the sender names from which the emails were transmitted were created using an automated process. (*See id*. at ¶¶ 60, 66(e)).

Argument

I. ZOOBUH HAS STANDING TO PURSUE CAN-SPAM CLAIMS GENERALLY AND AGAINST THE DEFENDANTS IN THIS MATTER.

It is well established that "any party, including the court *sua sponte*, can raise the issue of standing for the first time at any stage of the litigation." *New England Health Care Employees Pension Fund v. Woodruff*, 512 F.3d 1283, 1288 (10th Cir. 2008) (citing *Rector v. City and County of Denver*, 348 F.3d 935, 942 (10th Cir.2003)). Accordingly, ZooBuh, through this Memorandum, respectfully submits evidence to support its standing to pursue CAN-SPAM claims.

The CAN-SPAM Act states that a provider of Internet access service that is adversely affected by unlawful commercial email may bring a civil action in any district court of the United States with jurisdiction over the defendant. *See* 15 U.S.C. §7706(g)(1). Here, ZooBuh has standing to bring actions under CAN-SPAM because (a) ZooBuh is a *bona fide* Internet Access Service, and (b) ZooBuh is adversely affected by unlawful commercial emails, including the emails in question.

a. ZooBuh is a Bona Fide Internet Access Service

The CAN-SPAM Act defines Internet Access Service as "a service that enables users to access content, information, electronic mail, or other services offered over the Internet, and may also include access to proprietary content, information, and other services as part of a package of services offered to consumers. Such term does not include telecommunications services." *See* 15 U.S.C. § 7702(11) citing 47 U.S.C. § 231(e)(4). The Ninth Circuit, in *Gordon v. Virtumundo*, further limited standing to "*bona fide*" Internet Access Services, which it defined by citing to the Congressional Record in stating "[W]e intend that Internet access service providers provide

actual Internet access service to customers."[2] *See Gordon*, 575 F.3d 1040, 1050 (9th Cir. 2009) (citing 150 Cong. Rec. E72-02). Courts have extended the definition of Internet Access Services to "include[ ] traditional [ISPs], any email provider, and even most website owners." *MySpace, Inc. v. The Globe.com, Inc.*, No. 06-3391, 2007 WL 1686966, at *3 (C.D.Cal. Feb.27, 2007) (lodged herewith as **Exhibit 1**); *see also Facebook, Inc. v. ConnectU LLC,* 489 F.Supp.2d 1087, 1094 (N.D.Cal.2007).

Here, ZooBuh is a *bona fide* Internet Access Service. *See supra* Statement of Facts ¶¶ 4-14. Specifically, ZooBuh offers email services, blog hosting, and chat services to its customers. *Id*. ZooBuh has customers in all 50 states and in 27 different countries. *Id*. at ¶ 8. ZooBuh services approximately 35,000 customer accounts. *Id*. at ¶ 9. ZooBuh is widely recognized as a legitimate email provider and has been featured in various publications. *See id*. at ¶ 7. ZooBuh owns all the servers, routers, and switches on its network through which it hosts and provides its internet access services for its customers. *Id*. at ¶¶ 10, 14. Every ZooBuh email account is registered, hosted and serviced though ZooBuh's own hardware. *Id*. at ¶ 12. ZooBuh has sole ownership of all the hardware, complete and uninhibited access to the hardware, and sole physical control over the hardware. *Id*. at ¶ 14. ZooBuh also provides each of its customers with their own web-based email portal through which they access their selected web-based

[2] The plaintiff in *Gordon* did not qualify as an Internet Access Service despite providing email accounts because "Gordon [was] a registrant of a domain name, which he, through Omni, hosts on leased server space. He neither has physical control over nor access to the hardware, which GoDaddy owns, houses, maintains, and configures . . . . Gordon's service appears to be limited to using his "Plesk" control panel, which he accesses via an ordinary Internet connection through an ISP, to set up e-mail accounts and log-in passwords and to execute other administrative tasks. Verizon enables his online access. GoDaddy provides the service that enables ordinary consumers to create e-mail accounts, register domain names, and build personalized web pages. Gordon has simply utilized that service for himself and on behalf of others." *Gordon*, 575 F.3d at 1052.

services (e.g. email, blogs, chat.), which portal ZooBuh designed, controls, and maintains. *Id*. at ¶ 12.

For the reasons set forth above, ZooBuh is a bona fide Internet Access Service and qualifies for standing to assert actions under the CAN-SPAM Act.

b. ZooBuh was adversely affected by SPAM emails, including the emails in question.

As set forth in *Gordon*, the harm suffered by an Internet Access Service in order to establish standing under the "adverse affect" requirement of the CAN-SPAM Act "need not be significant in the sense that it is grave or serious, [but] must be of significance to a *bona fide* IAS provider-something beyond the mere annoyance of spam . . . ." *Gordon*, 575 F.3d at 1053-54. The court further explained that "[i]n most cases, evidence of some combination of operational or technical impairments and related financial costs attributable to unwanted commercial e-mail would suffice." *Id*. at 1054. Such impairments "include, but are not limited to, network crashes, higher bandwidth utilization, and increased costs for hardware and software upgrades, network expansion and additional personnel." *Id*. at 1053 (internal citations omitted).

Here, ZooBuh has experienced, and continues to experience on a daily basis, significant operational and technical impairments with related financial costs. *See supra* Statement of Facts at ¶¶ 15-31. Specifically, ZooBuh has experienced hardware crashes, server spikes, bandwidth spikes, kernel crashes, customer complaints, etc. *See id*. at ¶¶ 22-29. ZooBuh has also had to hire an additional employee whose sole job responsibility is to determine the source of SPAM emails to aid ZooBuh in stopping the emails permanently. *See id*. at ¶¶ 40-44.

The *Gordon* standard for standing does not require that a plaintiff prove that the emails at issue adversely affect the plaintiff, rather, that "[t]he e-mails at issue in a particular case . . .

contribute to a larger, collective spam problem." *See Gordon*, 575 P.3d at 1054. Here, approximately 70% of the email messages that ZooBuh receives on its system are unlawful commercial emails, of which the subject emails are a part. *See supra* Statement of Facts at ¶ 19. This number would be significantly higher if not for all the precautions that ZooBuh has taken. *See id*. In its ordinary course of business, ZooBuh utilizes SpamHaus, Razor, Pyzor and Spamassassin as a first line of defense for the unlawful emails received on its system. *See id*. at ¶ 15. Software such as Spamassassin identifies characteristics of the emails and also implements blacklists and DNS based spam block lists to block certain email senders. *See id*. at ¶¶ 16-17. To get around this, spammers create infinite numbers of internet domains from which to send SPAM, none of which accurately identify any party, and in some cases, are not domain names that actually exist. *See id*. at ¶ 20. These types of tricks, which alter the header information in an email message, help the emails to evade blacklists, spam filters, and help the emails to find their way onto ZooBuh's system. *See id*. These tricks also violate the CAN-SPAM Act. *See infra* Section II. The emails in question follow these trends and contain these characteristics as set forth below. *See supra* Statement of Facts at ¶¶ 38-46. If not for email of this nature, ZooBuh could successfully service all of its 35,000 customers through four servers. *See supra* Statement of Facts. at ¶ 11.

In summary, the unlawful emails that are ultimately harming ZooBuh's system, and which include the Better Broadcasting emails, are emails that are inherently deceptive, violate CAN-SPAM and that are tailored to evade the grasp of spam filters. In order to deal with spam problem, ZooBuh has, among other things, had to consistently increase the size and servicing capacity of its system. *See id*. at ¶ 18, 22. With each added server, ZooBuh has also had to

increase its bandwidth in order to service the new space adequately. *See id*. at ¶ 23. However, even with eight servers, ZooBuh consistently deals with server spikes and crashes, and the servers are pushed to capacity constantly, which significantly decreases the life span of the servers and is expensive in power consumption. *See id* at ¶ 24-25.

Though not required to prove standing, ZooBuh can demonstrate that the Better Broadcasting emails adversely affected it. Specifically, in May 2011, a month in which Defendants sent at least 2,366 unlawful commercial emails, ZooBuh experienced a primary DNS server overload which caused a crash and a bandwidth spike resulting in an 1800% increase above average usage. Fullmer Decl. at ¶ 51. In June 2011, a month in which Defendants sent at least 507 unlawful commercial emails, ZooBuh experiences a Mail server overload, which resulted in extremely slow delivery of legitimate emails and an eventual memory exhaustion which ended in an unrecoverable kernel crash. *Id*. at ¶ 52.

In each of the months, during which Defendants sent unlawful commercial emails to ZooBuh's customers, all of ZooBuh's servers were constantly running above their recommended capacity. *See id*. at ¶ 53. None of these spikes, crashes or delays would have occurred but for the unlawful emails to which Defendants' emails contributed. *See id*. at ¶ 54.

Recently, the Northern District of California, in *Facebook v. Power Ventures, In*c. ruled on a summary judgment motion that addressed standing. *See* 2012 WL 542586 (lodged herewith as **Exhibit 2**). In that decision, the court provided a very helpful analysis of the *Gordon* standard for standing.

There, the court determined that Facebook's receipt and analysis of approximately 60,000 messages constituted an adverse effect. *Id* at *5. It is worth noting that Facebook's network

consists of 901 million users and Facebook has over 3,000 employees. *See* Facebook Newsroom (lodged herewith as **Exhibit 3**). In that case, Facebook outlined its harm, with respect to the emails in question, as having to spend time and effort determining the source of the emails, and taking steps to get the emails to stop. *See Power Ventures*, 2012 WL 542586 at*4-5. The court held that Facebook did demonstrate an adverse effect, and that such was especially true because there were a documented 60,000 messages, and "the cost of responding to such a volume of spamming cannot be categorized as 'negligible.'" *Id.* at *5.

In this case, ZooBuh's network consists of approximately 35,000 users, ZooBuh has three employees, and there are 13,453 emails at issue. *See* Fullmer Decl. at ¶¶ 8, 11, 45. Accordingly, the subject emails created a significantly greater burden for ZooBuh than the 60,000 email received by Facebook's 901 million users and over 3,000 employees. Similar to Facebook, for each email, ZooBuh had to expend man hours and work to identify the source, to examine the transmission information, to examine and analyze the header information, to take efforts to determine how and why the specific emails were able to circumvent and/or bypass preliminary filtering techniques, and to ultimately attempt to make the emails stop. *See supra* Statement of Facts at ¶¶ 33-37. As stated in *Facebook v. Power Ventures*, ZooBuh has standing to pursue CAN-SPAM claims against Defendants because the documented expenditure related to ZooBuh's attempts to identify and block the subject emails cannot be categorized as negligible and therefore confer standing. *See Power Ventures*, at *5.

The harm suffered by ZooBuh is much more significant than the mere annoyance of having to deal with SPAM or the process of dealing with SPAM in the ordinary course of business (i.e. installing a spam filter to flag and discard spam). The harm ZooBuh suffers is

manifested in significant financial expense and burden, significant loss of time, significant loss in profitability and ability to grow the company, as well as creating significant decreases in the life span of ZooBuh's hardware, which ultimately will mean more spikes, more crashes, and premature hardware replacements resulting in more expenses. *See supra* Statement of Facts at ¶ 31. Accordingly, ZooBuh has standing to pursue CAN-SPAM claims generally and against the Defendants in this matter.

II. THE EMAILS CONTAIN SIGNIFICANT WILLFUL CAN-SPAM VIOLATIONS

The CAN-SPAM Act makes it unlawful for any person to initiate the transmission of a commercial electronic mail message, or a transactional or relationship message, that contains, or is accompanied by, header information that is materially false or materially misleading ("**Header Violations**"). *See* 15 U.S.C. 7704(a)(1).

Additionally, the CAN-SPAM Act dictates that "it is unlawful for any person to initiate the transmission of any commercial electronic mail message to a protected computer unless the message provides (i) clear and conspicuous identification that the message is an advertisement or solicitation; (ii) clear and conspicuous notice of the opportunity under paragraph (3) to decline to receive further commercial electronic mail messages from the sender; and (iii) a valid physical postal address of the sender." ("**Content Violations**"). 15 U.S.C. 7704(a)(5). Here, the subject emails contain both (a) Header Violations and (b) Content Violations.

a. The emails violate both 15 U.S.C. 7704(a)(1) and 15 U.S.C. 7704(a)(1)(A) which constitute Header Violations.

Very few decisions have issued regarding Header Violations under CAN-SPAM. To date, there is not one published opinion in the Tenth Circuit or in any District Court within the

Tenth Circuit that addresses any aspect of CAN-SPAM. Accordingly, there is a great need for this Court to issue a Memorandum Decision for publication regarding these points.

First, the emails violate 15 U.S.C. 7704(a)(1). There are several decisions arising out of Default Judgment and Summary Judgment proceedings wherein the Court awarded damages for Header Violations. In those cases, the Court determined that Header Violations existed where: the emails failed to identify that they came from defendant (the sender was identified in the publicly available WHOIS information). *See Tagged, Inc. v. DOES 1 through 10*, 2010 WL 370331 (N.D. Cal.) (lodged herewith as **Exhibit 4**); the emails did not accurately identify any party. *See Facebook v. Wallace*, 2009 WL 3617789 (N.D. Cal.) (lodged herewith as **Exhibit 5**); and, the emails contained inaccurate sender names (i.e. identifying "facebook" as the sender when the sender was not related to Facebook). *See Power Ventures*, 2012 WL 542586 (N.D. Cal.). Though these decision are helpful, they do not provide much analysis or direction. Accordingly, it is helpful to look outside of CAN-SPAM for direction on the interpretation of the statute.

California Business and Professions Code § 17529.5(a)(2) is substantially similar to § 7704(a)(1) of CAN-SPAM in that it prohibits commercial email which "contains or is accompanied by falsified, misrepresented, or forged header information." Cal. B&P Code § 17529.5(a)(2). Though the language is similar, due to the federal preemption doctrine, the California code has been defined as prohibitive of "deceptive" header information only, thereby creating a more onerous burden on a plaintiff than the "misrepresentation" standard in CAN-SPAM and avoiding pre-emption by the CAN-SPAM Act. *See Hypertouch v. Valueclick, Inc.*,

192 Cal.App.4th 805, 825-830 (2011); *Asis Internet Services v. Subscriberbase Inc.*, 2010 WL 1267763 (N.D. Cal.) (lodged herewith as **Exhibit 6**).

In consideration of the California Code's more onerous burden, the recent California appellate decision in *Balsam v. Trancos* offers guidance on what constitutes a Header Violation under CAN-SPAM. 2012 WL 593703 (Cal. Ct. App.) (lodged herewith as **Exhibit 7**).

In *Trancos*, the plaintiff sued an email marketer, similar to Defendants in this case, for sending eight commercial email advertisements on behalf of companies that hired the defendant. *Id*. at *2. Before sending the emails, the email marketer privately registered the domains it used to send the emails with a proxy service (i.e. eNom, Moniker, etc.). *Id*. at *6. The proxy service, in turn, displayed the proxy service's contact information on the domain name registration records instead of the defendant's contact information. *Id*. at *6-7. Accordingly, a recipient seeking to determine who sent the emails could not determine the sender because the domains were cloaked and a WHOIS look-up (a publicly available service that allows users to determine persons associated with domain names) would reveal the proxy service's contact information and not that of the defendant. *Id*.

The appellate court applied CAN-SPAM's definition of header information and, noting CAN-SPAM's parallel provision to B&P Code § 17529.5(a)(2), the Court agreed that where the domain names in the emails did not represent a real company and could not be readily traced back to the sender, through available public databases such as WHOIS, such constituted falsification or misrepresentation for purposes of the statute. *Id*. at *10. As to privately registered domain names, the Court held "where, as in this case, the commercial e-mailer intentionally uses privately registered domain names in its headers that neither disclose the true

sender's identity on their face nor permit the recipient to readily identify the sender . . . such header information is deceptive and does constitute a falsification or misrepresentation of the sender's identity," thereby meeting the more strict standard of the California Code. *Id*. at * 7.

Here, 13,333 of the emails meet the *Trancos* deception standard in that they contained a generic or nonsensical "from" line and domain name, and also originated from a privacy protected domain. *See* Ringwood Decl. at ¶¶ 6-7. Examples of the "from" lines include "Accounting Degree", "Add a Sunroom", "Adult Education", "Air Conditioner", "Airline Tickets", "Ink Cartridges", "Ultrasound Technician" (a complete list of "From" is attached as Exhibit C to Fullmer Decl.).

When ZooBuh sought to identify the emailer through the publicly available WHOIS database, the WHOIS database record displayed the proxy service's contact information on the domain name registration records instead of the emailer's contact information, thereby preventing ZooBuh from identifying the emailer. *See supra* Statement of Facts at ¶ 45; *see also* WHOIS Records, attached as Exhibit A to Ringwood Decl. None of the 13,333 contained a "From" line that actually identified any party, and therefore did not satisfy the safe harbor provision of 7704 (a)(1)(B).

Because the California anti-spam statute has not been preempted, prohibits deception, and imposes a more onerous burden on a plaintiff that does the CAN-SPAM Act, this Court can reasonably extend the *Trancos* analysis to CAN-SPAM header violations. Under this standard which, based on the preemption doctrine, poses a more strict standard than the CAN-SPAM Act, 13,333 of the emails violate 15 U.S.C. 7704(a)(1) in that they are false and/or misleading.

Second, the emails violate 15 U.S.C. 7704(a)(1)(A). Header Violations under CAN-SPAM are not limited to false or misleading header information. Under 7704(a)(1)(A), even header information that is technically accurate violates the CAN-SPAM Act when the email "includes an originating electronic mail address, domain name, or Internet Protocol address the access to which for purposes of initiating the message was obtained by means of false or fraudulent pretenses or representations." 15 U.S.C. 7704(a)(1)(A).

Here, 13,452 of the emails originated from sender domain names registered with the eNom, and one email originated from a sender domain registered with Moniker. *See supra* Statement of Facts at ¶ 43. Each of these registrars requires the party registering the domain to accept their Terms and Conditions. The Terms and Conditions of each registrar contain a provision whereby the registrant indicates that they will not use the domain name for purposes of sending unlawful commercial email or SPAM. *See* eNom Registration Agreement and Abuse Policy, attached as Exibit E to Fullmer Decl.; *see also* Moniker Registration Agreement, ¶ 10, attached as Exhibit F to Fullmer Decl. Accordingly, in order to obtain the domain names used to send the emails in this case, the Defendants represented to the domain registrars (in this case eNom and Moniker) that the domain names would not be used for SPAM purposes. However, the domain names were intended to be used, and were used, for SPAM purposes. Consequently, the Defendants obtained the sender domains, from which they sent 13,452 emails, under false and fraudulent pretenses in violation of 7704(a)(1)(A).

b. The emails violate 15 U.S.C. 7704(a)(5) which constitutes Content Violations.

The CAN-SPAM Act dictates that "it is unlawful for any person to initiate the transmission of any commercial electronic mail message to a protected computer unless the

message provides (i) clear and conspicuous identification that the message is an advertisement or solicitation; (ii) clear and conspicuous notice of the opportunity under paragraph (3) to decline to receive further commercial electronic mail messages from the sender . . . ." (collectively "**Required Content**"). 15 U.S.C. 7704(a)(5). The CAN-SPAM Act provides statutory damages against parties who engage in a pattern or practice in violation of these provisions. *See* 15 U.S.C. 7706(g)(3)(A).

"Clear and Conspicuous" in commercial communication through an electronic medium is defined as follows: the "disclosure must be unavoidable . . . [and] any visual message shall be of a size and shade, with a degree of contrast to the background against which it appears, and shall appear on the screen for a duration and in a location sufficiently noticeable for an ordinary consumer to read and comprehend it." *F.T.C. v. Affiliate Strategies, Inc.*, 2011 WL 3300097, *2 (D. Kansas) (emphasis added) (lodged herewith as **Exhibit 8**).

As set forth in the Letter of Opinion, the only possible method through which it can be certain that the Required Content would display for the recipient would be to provide it in text in the email body. *See* Letter of Opinion at ¶¶ 38-43. Accordingly, in order for the Required content to be "unavoidable" and appear on the screen for a duration and in a location sufficiently noticeable for an ordinary consumer to read and comprehend it, the Required Content must be provided in the plain text of the email. *See id*.

Here, none of the Required Content was provided in the text of the emails. *See id*. at ¶¶ 61-65, 67-70. Further, it does not appear that the Required Content was provided in any format (i.e. HTML, remotely hosted images, etc.). Nevertheless, if the Required Content was provided, it would have been through remotely hosted images, which images would be blocked by the

majority, if not all, email clients (a fact commonly known by anyone familiar with email technology, including email marketers), which images would only exist for a short time on a third party server, and which images would not likely be viewed by a recipient. *See id*. at ¶¶ 62-25, 67-70. Accordingly, the emails did not contain "clearly and conspicuously displayed" Required Content and violate 15 U.S.C. 7704(a)(5).

III. DAMAGE CALCULATION

Under the CAN-SPAM Act, a plaintiff may elect to recover monetary damages in an amount equal to the greater of actual losses or statutory damages. *See* 15 U.S.C. 7706(g)(1)(B). It is well established that "[a] plaintiff may elect statutory damages regardless of the adequacy of the evidence offered as to his actual damages and the amount of the defendant's profits . . . and if statutory damages are elected, the court has wide discretion in determining the amount of statutory damages to be awarded, constrained only by the specified maxima and minima." *Facebook. v. Wallace*, 2009 WL 3617789 at *2 (citing *Columbia Pictures Television, Inc. v. Krypton Broad. of Birmingham, Inc.*, 259 F.3d 1186, 1194 (9th Cir. 2001) (internal quotations omitted).

In this case, ZooBuh has elected to recover statutory damages pursuant to 15 U.S.C. 7706(g)(3)(A) which are calculated by multiplying the number of violations by up to $100 in the case of a Header Violations and up to $25 in the case of a Content Violations. *See* 15 U.S.C. 7706(g)(3)(A). Further, the Court can award treble damages where the defendant "use[d] scripts or other automated means to register for multiple electronic mail accounts or online user accounts from which to transmit to a protected computer, or enable another person to transmit to

a protected computer, a commercial electronic mail message." *See* 15 U.S.C. 7704(b)(2); 15 U.S.C. 7706(g)(3)(C).

In *Wallace*, the court awarded the plaintiff $710,737,650 in damages. 2009 WL 3617789 at *2. The damage award was calculated by multiplying the number of emails by "$50.00 per violation of the CAN-SPAM Act." *See id*. In determining to award $50.00 per violation, the court looked at various factors. Specifically, the court stated that "[t]he record demonstrates that Wallace willfully violated the statutes in question with blatant disregard for the rights of Facebook and the thousands of Facebook users whose accounts were compromised by his conduct." *Id*. Wallace's conduct included violating a TRO and preliminary injunction. *See id*. Though the defendants actions were sever, the court did not believe that the actions merited an award in excess of seven billion dollars. *See id*. Accordingly, instead of awarding the full $100 per violation and treble damages, the court scaled back its award to $50 per violation.

In *Tagged*, the court awarded the plaintiff $151,975 for 6,079 emails sent by the defendant. *See Tagged, Inc. v. Does 1 through 10*, 2010 WL 370331, *12 (N.D. Cal.). There, the court did not grant $50 per email, as in the *Wallace* case, because the defendant sent only 6,079 emails as compared to the millions of spam messages sent in the *Wallace* matter. *See id*. at 11.

In *Asis Internet Services v. Rausch*, the Court awarded the plaintiff $865,340.00 for various violations of 15 U.S.C. 7704(a)(1) (which carries an up to $100 penalty) and 15 U.S.C. 7704(a)(2) (which carries up to a $25 penalty). *See* 2010 WL 1838752, *7-8 (N.D. Cal.) (lodged herewith as **Exhibit 9**). Specifically, the court awarded $25 per violation of 15 U.S.C. 7704(a)(1) and $10 per violation of 15 U.S.C. 7704 (a)(2). As with the *Tagged* decision, the

court compared the case to *Wallace* and stated that "[t]his case involves far fewer emails than in [*Wallace*]." *Id* at *7. Further, the defendant "did not willfully violate an injunction" as was the case in *Wallace*. *Id*. After pronouncing the base award, the court considered the evidence that the defendant had also engaged in dictionary attacks and automated scripting in violation of 15 U.S.C. 7704(b). *See id*. at *8-9. Based on that fact, the court awarded treble damages as allowed by the statute for a total damage award of $2,596,020.00. *See id*. at *9.

The instant case is most similar to *Asis*. Here, there are 13,453 commercial emails in question that each contain one or more willful violations of the CAN-SPAM Act. Specifically, there are 13,333 emails that violate 15 U.S.C.(a)(1) (which carries an up to $100 penalty), 13,453 emails that violate 15 U.S.C.(a)(1)(A) (which carries an up to $100 penalty), and 13,453 emails that violate 15 U.S.C. 7704(a)(5) (which carries up to a $25 penalty). The emails also contain significant evidence of other spamming practices, which illustrate the willful nature of the violations (i.e., registration of many .info domain names, image tracking, Bayes Poisoning, scripting). *See* Letter of Opinion at ¶¶ 52-66. Accordingly, this Court should adopt the *Asis* standard and award at least $25 per violation of 15 U.S.C. 7704(a)(1) and 7704(a)(1)(A), and at least $10 per violation of 15 U.S.C. 7704(a)(5) for a total base damage award of $804,180.00 jointly and severally against the Defendants.

Additionally, there is significant evidence that the Defendants used an automated process through which to create the sender email addresses from which to send the emails in question. *See id*. at ¶¶ 60, 66(d). Specifically, the sender email addresses, when viewed alphabetically, demonstrate a pattern of words selected in an ascending alphabetical order. *See id*. at ¶ 66(d).

Additionally, some of the words cross domain names, indicating that the same script generated the domains by using a dictionary file. *See id*.

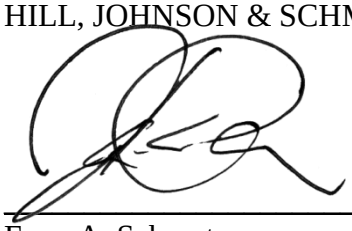
Such practices violate 15 U.S.C. 7704(b) and entitle a plaintiff to treble damages. *See* 15 U.S.C. 7704(b)(2); 15 U.S.C. 7706(g)(3)(C). Accordingly, this Court should adopt the *Asis* standard with respect to aggravated damages, and should award treble damages in this case, for a total damage amount of $2,412,540.00 jointly and severally against the Defendants.

Conclusion

Based on the foregoing, ZooBuh respectfully requests that this Court find that ZooBuh is a bona fide Internet access service with standing to pursue CAN-SPAM claims, and that ZooBuh was adversely affected by SPAM in general, including the Better Broadcasting emails. ZooBuh further requests that this Court find that the emails violated 15 U.S.C. 7704(a)(1), 15 U.S.C. 7704(a)(1)(A), 15 U.S.C. 7704(a)(5), and 15 U.S.C. 7704(b)(2), and respectfully requests that this Court award at least $2,412,540.00 in damages for the willful violations of the CAN-SPAM Act that exist in the emails sent by Better Broadcasting.

DATED this 1st day of June, 2012.

HILL, JOHNSON & SCHMUTZ, LC



Evan A. Schmutz
Wm. Kelly Nash
Jordan K. Cameron
Attorneys for Plaintiff